IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

UNITED STATES OF AMERICA	§	
	§	
v.	§	No. 3:09-CR-210-B
	§	
JESSE WILLIAM MCGRAW (1)	§	

GOVERNMENT'S RESPONSE TO MCGRAW'S MOTION
FOR BILL OF PARTICULARS

The United States of America respectfully files this response in opposition to McGraw's Motion for Bill of Particulars.

MCGRAW IS NOT ENTITLED TO A BILL OF PARTICULARS

1. McGraw complains that he cannot prepare a defense without knowing (1) the description of the particular computers compromised, (2) the description of the malicious programs, codes, and commands used, (3) how the damage occurred, (4) the defendant's thought-process while committing the offenses, and (5) the exact dates and times of the computer compromises. However, McGraw has received all that information and more from the indictment, discussions with the government, a proposed factual resume, and the extensive discovery provided to the defense.

2. A defendant does not have a right to a bill of particulars. *Wong Tai v. United States*, 273 U.S. 77, 82 (1927); *United States v. Burgin*, 621 F.2d 1352, 1358 (5th Cir.1980). It is in the discretion of the court whether to order the filing of a bill of particulars. *United States v. Gorel*, 622 F.2d 100, 104 (5th Cir.1979). "The purpose of a

bill of particulars is to inform an accused of the charge with sufficient precision to reduce trial surprise, to enable adequate defense preparation, and critically, by the fleshing out of the charges to illuminate the dimensions of jeopardy." *United States v. Davis*, 582 F.2d 947, 951 (5th Cir.1978). McGraw currently has reviewed and/or possesses almost all of the physical evidence the government intends to present at trial. The only physical evidence McGraw has not received are any diagrams, charts and graphs the government may create for trial; any additional physical evidence that may be received in response to trial subpoenas; and any physical items a witness may bring with him/her when he/she appears for a pretrial interview or for trial.

THE INDICTMENT IS SUFFICIENT

3. McGraw is charged by a two count indictment with violations of 18 U.S.C. §1030(a)(5)(A), which makes it a felony for a person to

> knowingly cause[] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally cause[] damage without authorization, to a protected computer.

4. The sentencing provisions for a violation of §1030(a)(5)(A), as alleged in the indictment, are found in §1030(c)(4)(B)(i)(II) and (IV):

> The punishment for an offense under subsection (a) . . . of this section is . . . a fine under this title, imprisonment for not more than 10 years, or both, in the case of — (i) an offense under subsection (a)(5)(A), which does not occur after a conviction for another offense under this section, if the offense caused . . .
>
> > (II) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals; [or]

(IV) a threat to public health or safety.

5. The instant indictment tracked the statute and accused McGraw of "knowingly caus[ing] the transmission of a program, code, and command, and as a result of such conduct, intentionally caus[ing] damage without authorization to a protected computer." Pursuant to §1030(e)(8), damage "means any impairment to the integrity or availability of data, a program, a system, or information."

6. The government advised the defense that at least fourteen[1] computers had been compromised by McGraw. Two of the fourteen computers accessed and compromised by McGraw provided a basis for the two count indictment. Count One did identify a computer compromised by McGraw, as being "owned by the Carrell Clinic, located at 9301 North Central Expressway, Dallas, Texas; [and] used to maintain patient medical records for the diagnosis and treatment of the Carrell Clinic patients." Count One further provided the following allegation to satisfy the sentencing provision in §1030(c)(4)(B)(i)(II).

> McGraw transmitted a malicious program, code, and command that gave McGraw the potential to modify and impair medical examinations, diagnoses, treatments, or care of one or more individuals.

7. Count Two did identify a computer compromised by McGraw, as "owned by the North Central Surgery Center and other tenants in the Carrell Clinic building, located at 9301 North Central Expressway, Dallas, Texas; [and] a HVAC computer controlling the

[1] McGraw accessed without authorization and transmitted a program, code, and command into at least fourteen "desktop" computers, and one laptop.

heating, ventilation, and air conditioning for the North Central Surgery Center and other tenants." Count Two further provided the following allegation to satisfy the sentencing provision in §1030(c)(4)(B)(i)(II) and (IV).

> McGraw transmitted a malicious program, code, and command that gave McGraw the potential to modify the operations of the building HVAC system resulting in the impairment of patient medical examinations, diagnoses, treatments, or the care of one or more individuals, and threatened public health and safety.

8. As it applies to the instant case, a program, code, or command is malicious if it is unauthorized and has an adverse effect, such as causing the loss of confidentiality, integrity, availability, usability, performance, or reliability[2].

A BILL OF PARTICULARS IS NOT WARRANTED

9. The indictment sufficiently describes the crimes with which McGraw is charged. McGraw's indictment only relates to two of at least fourteen computers compromised by McGraw. At trial, the government intends to introduce evidence of the totality of McGraw's unauthorized accesses and compromises of the computers within the Carroll Clinic Building. In his motion, McGraw seems to want a tutorial of the government's case. The details requested by McGraw primarily relate to the evidence to be presented during trial, not simply the essential elements of the offense charged.

10. A bill of particulars is not a proper tool for discovery, see *Davis*, 582 F.2d at 951, and should not to be used to provide detailed disclosure of the government's evidence

---

[2] National Security Agency's *Guidance for Addressing Malicious Code Risk*, § 2.1.1 Sept. 10, 2007.

prior to trial. *United States v. Kilrain*, 566 F.2d 979, 985 (5th Cir.1978). Neither should it be used to compel the government to provide a detailed explanation of its trial strategy or legal theories. *Burgin*, 621 F.2d at 1358.

11. A bill of particulars should not be used to ascertain the Government's theory "as to the means by which a defendant committed a specific criminal act." *United States v. Drabovskiy,* 2009 WL 2969902 (WDLA, Sept. 10, 2009).

MCGRAW CANNOT CLAIM SURPRISE

12. Denial of a motion for a bill of particulars "will be reversed only if the denial of the bill was a clear abuse of discretion ... [and] [s]uch abuse will be found only if it appears that the accused was actually surprised at trial and that his rights were substantially prejudiced by the denial." *U.S. v. Vasquez*, 867 F.2d 872, 874 (5th Cir.1989). If the Government "provides the requested information called for in some other satisfactory form, then no bill of particulars is required." *Id. See United States v. Kirkham*, 129 Fed.Appx. 61, 72 (5th Cir. 2005) (affirming denial of bill of particulars where the government provided the defendants "with voluminous discovery.")

13. The government provided extensive discovery to McGraw's defense team, producing copies of documents, photographs, and digital data, and making available for review all of the physical items seized. The government also met in person with McGraw's attorney and his computer forensic analyst, and discussed the evidence establishing McGraw's guilt. McGraw's defense team currently possesses, among other

items and data, the following;

a. Records from McGraw's employer, United Protection Service, showing that from November 1, 2008, to June 26, 2009, McGraw was assigned to work as a security guard for the Carrell Clinic building (CC Bldg), and worked a shift from 11 p.m. to 7 a.m.

b. McGraw's handwritten statement admitting to repeated unauthorized accesses to the computers and the theft and use of a computer from the CC Bldg; and McGraw's handwritten notes identifying his email accounts and various website memberships and screennames, to include his Logmein.com account.

c. McGraw's self-recorded videos, including one video made and narrated by McGraw while on duty in the CC Bldg, showing McGraw's accessing a computer without authorization on the 5th floor, and transmitting at least one malicious program, code, and command into the computer.

d. Digital data from McGraw's personal laptop and from a stolen laptop used by McGraw, from which he remotely accessed some of the compromised computers in the CC Bldg.

e. Log records from Computrace.com, showing the use of the stolen laptop by McGraw from January 14, 2009 through March 30, 2009.

f. Log records from McGraw's account at Logmein.com, showing that McGraw remotely accessed without authorization at least 11 of the 14 compromised computers, between March 17, 2009 and June 23, 2009.

g. Data from IT personnel responsible for remediating the compromised computers in the CC Bldg, showing that all 14 of the compromised computers contained the unauthorized program Logmein.

h. Records from a previously installed keystroke logger on the HVAC computer from the CC Bldg showing, among other things, the following activity by McGraw while physically at the HVAC computer on December 12 and 13, 2008:

(1) McGraw without authorization accessed the HVAC computer: began the download of "Ophcrack-vista-livecd-2.1.0.iso" a malicious password

cracking tool from the website sourceforge.net and downloaded and installed without authorization Team Viewer 4, a remote access program.

(2) McGraw circumvented the security software McAfee and added Team Viewer to the list of allowed programs in McAfee.

(3) McGraw without authorization again accessed the HVAC computer, inserted a recoverable storage device named "HARD DISK X," and executed the program daemon4301-lades which allowed McGraw to emulate a CD/DVD device with the recoverable storage device. McGraw then attempted to use "Sonic Record Now," a CD/DVD burning software, to create a bootable CD image using the previously downloaded "OphCrack-xp-livecd.iso".

i. Records from McGraw's account at photobucket.com, showing, among other things, that on December 20, 2008, McGraw uploaded 3 screenshots of the HVAC computer from the CC Bldg.

j. Records from the keystroke logger installed on the HVAC computer from the CC Bldg showing that on April 13, 2009, McGraw without authorization remotely accessed the HVAC computer using the password "pred818" and downloaded and installed the malicious program "Cain & Abel v4.9.29," a key stroke logger and network traffic sniffer. McGraw then started the "Cain" software and accessed the HVAC computer's Local Security Authority, also known as "LSA secrets," where cached user authentications are stored on the HVAC computer.

k. Physical items seized from McGraw, his car, or his house, to include, but not limited to, the following items displayed by McGraw in his self-recorded videos:

(1) a disk containing OphCrack;

(2) false FBI credentials; and

(3) a cell phone jammer.

l. Physical items seized from McGraw, his car, or his house, to include, but not limited to, notebooks containing instructions as to how to hack into computers and computer systems.

14. In September 2009, the government provided McGraw with a proposed factual resume, specifically detailing the facts intended to support a guilty plea. A copy of the proposed factual resume is attached hereto as Exhibit 1.

Respectfully submitted,

JAMES T. JACKS
United States Attorney

S/ Candina S. Heath
CANDINA S. HEATH
Assistant United States Attorney
Texas State Bar. No. 09347450
1100 Commerce Street, 3d Floor
Dallas, Texas 75242
Telephone: 214.659.8600

CERTIFICATE OF SERVICE

I hereby certify that on January 19, 2010, I electronically filed the foregoing document with the clerk for the U.S. District Court, Northern District of Texas, using the electronic case filing system of the court. The electronic case filing system sent a "Notice of Electronic Filing" to John Nicholson, attorney for McGraw, who consented in writing to accept this Notice as service of a document by electronic means.

S/ Candina S. Heath
CANDINA S. HEATH
Assistant United States Attorney